

REMARKS

Claims 4, 6-8 and 10-12 are pending in this application. Claims 4, 8 and 10 have been amended in this response. Claims 5, 7 and 9 have been cancelled, without prejudice. No new matter has been introduced. Favorable reconsideration is respectfully requested.

Claims 4-6 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicant respectfully traverses the rejection. In light of the amendments submitted above, Applicant posits that the claimed features result in a practical application that produces a concrete, useful and tangible result to form the basis of statutory subject matter pursuant to 35 U.S.C. §101. Withdrawal of the rejection is respectfully requested.

Claims 4-6, 8, and 12 were rejected under 35 U.S.C. §102(e) as being anticipated by *Mittra* (US Patent 5,748,736). Claims 7 and 9-11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Mittra* (US Patent 5,748,736) in view of *Schneier* (Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C, 1996 pgs. 34-41). Applicant respectfully traverses this rejection, because the cited reference, alone or in combination, do not disclose or suggest features of the present invention as described in independent claims 4, 8 and 10.

As argued previously, the present invention authenticates in three steps for identifying the device by means of device-specific information, authenticating the device by means of a group-specific information, and achieving compliance between the identified and the authenticated device which were performed by the communication partner of the device. In the present invention, the key device B identifies the key device A by receiving the certificate $Z(A)$ from the key device A, which is a device-specific information characterizing the identity of key device A. The key device B authenticates the key device A (i.e., determines the membership of key device A to the group of certified key devices) by decrypting the signature $S(Z(A))$ (i.e., the device-specific information about the membership of key device A to the group of certified key devices) by means of the public key pAD (i.e. the group-specific information). The key device B achieves compliance between the identified and the authenticated devices by comparing the received certificate $Z(A)$ (i.e., the identity characterizing information of the key device A) with the certificate $Z(A)$ derived from the signature $S(Z(A))$ (i.e., the authentication characterizing

information of the device A to the group of certified key devices) by means of the group-specific information public key pAD.

The present claims recite a method of source authentication in a communication group, whereby the authentication can only be performed by members of the communication group. One objective defined in the claims is to encrypt and decrypt the device-specific certificate with a group-specific public-private key. An administrator in a communication group would typically hold a group-specific secret key sAD and send the corresponding group-specific public key pAD to each member of the communication group in an initialization phase. In the initialization phase, the administrator also sends a device-specific certificate Z(A) and a corresponding device-specific signature E(Z(A),sAD) being the signed certificate of the device in the communication group. Device A in the communication group transmits a message combined with the device-specific certificate Z(A) and the corresponding device-specific signature E(Z(A),sAD) to another device B in the communication group. The other device B verifies the received device-specific signature E(Z(A),sAD) by decrypting the device-specific signature E(Z(A),sAD) with the group-specific public key pAD corresponding to the relationship defined as:

$$D(S(Z(A)), pAD) = D(E(Z(A), sAD), pAD) = Z(A)$$

and compares the decrypted device-specific signature

$$(S(Z(A)), pAD) \text{TD} (E(Z(A), sAD), pAD)$$

i.e. the device-specific certificate Z(A), with the received certificate. When a match is identified between the device-specific signature E(Z(A),sAD) and the device-specific certificate Z(A) corresponding to relationship defined above, the device B recognizes the origin of the received message being a message of the group device A. Thus the authentication of the received message is guaranteed.

In contrast, *Mittra* discloses a method and a system for secure communication between several devices via multicast. Each device receives a digitally signed certificate characterizing its identity from a Group Security Controller (GSC) (column 11, lines 34 to 37). *Mittra* is silent

regarding the type of signature or encryption used in the application. More importantly, *Mittra* does not encrypt the signature by a private-public-key. Furthermore, the GSC does not send a certificate combined with a digitally signed certificate to each device as required in the present claims. The authentication in *Mittra* is based on a certificate assigned to each member of the communication group, and the certificate is signed with a general-purpose signature, that ultimately burdens each communication device with obtaining the key for decryption of each signature (see col. 8, lines 22-31). *Mittra* teaches the use of public key algorithms (col. 9, line 48-col. 10, line 62), however, the disclosure requires that a specific key must be exclusively chosen for encrypting the data, and thus does not teach the features claimed above. In col. 9, line 48 to col. 10, line 62, *Mittra* merely teaches (1) multicasting of a group key; (2) multicasting a sender key authenticated by the GSC over a secure channel; and (3) multicasting a random key chosen by the sender, authenticated by the GSC over a secure channel. Accordingly, *Mittra* does not disclose or teach “assigning each key device a group-specific public key, wherein a group comprised of a limited total number of key devices; assigning each key device a group-specific signature of the device-specific certificate;” and “establishing a link between at least two key devices transmitting a corresponding device-specific certificate and a corresponding device-specific signature from one of the key devices to another one of the key devices, wherein the other one of the key devices verifying authenticity of the corresponding device-specific certificate” as recited in the present claims. Accordingly it is respectfully submitted that the rejection under 35 U.S.C. §102(e) is improper and should be withdrawn.

Regarding *Schneier*, the reference teaches that the signing of documents is performed by signing the hash function of the document with public-private cryptography. In *Schneier* a signed hash function of a document is transmitted. However, *Schneier* does not disclose the transmitting of a device-specific certificate and of a corresponding device-specific public key as recited in claim 4, and certainly does not disclose the verification relationship discussed above.

Finally, there is no teaching, suggestion or motivation to combine *Mittra* and *Schneier*, as *Schneier* only discloses a public-private cryptology for signing a document with its hash function. A method for performing the authentication only by members of the communication group is not disclosed at all in *Schneier*. *Schneier* discloses a general public key that is

associated with a particular user's private key. *Schneier* does not disclose assigning group-specific keys, which perform a different function from a generalized public key.

A person of ordinary skill in the art would not be motivated to combine *Schneier* with *Mitra* in the manner suggested by the Office Action. *Mitra* specifically deals with multicasting of group keys (Kgrp) or sender keys that are exclusively selected from the GSC (i.e., on or the other, but not both) during a multicast (see col. 9, line 59 – col. 10, line 62). However, using the disclosure in *Schneier*, it is expressly taught the usage of the GSC would be obviated using the configuration disclosed therein (see page 37, last paragraph). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). The initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985). When the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of the teachings is proper. *Ex parte Skinner*, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1986). (see MPEP 2142).

Further, the Federal Circuit has held that it is "impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." *In re Fritch*, 23 U.S.P.Q.2d 1780, 1784 (Fed. Cir. 1992). "One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention" *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

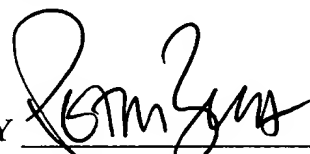
Moreover, the Federal Circuit has held that "obvious to try" is not the proper standard under 35 U.S.C. §103. *Ex parte Goldgaber*, 41 U.S.P.Q.2d 1172, 1177 (Fed. Cir. 1996). "An-obvious-to-try situation exists when a general disclosure may pique the scientist curiosity, such that further investigation might be done as a result of the disclosure, but the disclosure itself does not contain a sufficient teaching of how to obtain the desired result, or that the claim result would be obtained if certain directions were pursued." *In re Eli Lilly and Co.*, 14 U.S.P.Q.2d 1741,

1743 (Fed. Cir. 1990). Accordingly, it is respectfully submitted that the rejection under 35 U.S.C. §103(a) is improper and should be withdrawn.

In light of the above amendments and arguments, Applicant respectfully submits that claims 4, 6-8 and 10-12 are now in condition for allowance, which is respectfully requested. A petition for a two month extension of time, along with a check in the amount of \$450.00 is enclosed herein. As March 19, 2005 fell on a Saturday, no further extensions are required. If any additional fees are due in connection with this application as a whole, the Examiner is authorized to deduct such fees from deposit account no. 02-1818. If such a deduction is made, please indicate the attorney docket no. (0114131-002) on the account statement.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY 

Peter Zura
Reg. No. 48,196
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690-1135
Phone: (312) 807-4208

Dated: March 21, 2004